Schéma Français

la Sécurité des Technologies de

Ce document constitue le rapport de certification du produit “Micro-circuit ATMEL AT90SC6464C (référence AT568A9 rév. F)”.

Ce rapport de certification est disponible sur le site internet de la Direction Centrale de la Sécurité des Systèmes d'Information à l'adresse suivante :

www.ssi.gouv.fr

Toute correspondance relative à ce rapport de certification doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d’Information
Bureau Certification
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

certification.dcssi@sgdn.pm.gouv.fr

Ce document est folioté de 1 à 20 et certificat.

PREMIER MINISTRE

Schéma Français d'Évaluation et de Certification de la Sécurité des Technologies de l'Information

CERTIFICAT 2001/14

Micro-circuit ATMEL AT90SC6464C (référence AT568A9 rév. F)

Développeur : ATMEL Smart Card ICs

EAL1 Augmenté

Commanditaire : ATMEL Smart Card ICs

Le 24 août 2001,

Le Commanditaire :
Le Directeur de la division ATMEL Smart Card ICs
Lucien BRAU

L'Organisme de certification :
Le Directeur Central de la Sécurité des Systèmes d'Information
Henri SERRES

Ce produit a été évalué par un centre d'évaluation de la sécurité des TI conformément aux Critères Communs pour l'évaluation de la sécurité des TI version 2.1 et à la méthodologie commune pour l'évaluation de la sécurité des TI version 1.0.

Ce certificat ne s'applique qu'à la version évaluée du produit dans sa configuration d'évaluation et selon les modalités décrites dans le rapport de certification associé. L'évaluation a été conduite en conformité avec les dispositions du Schéma français d'évaluation et de certification de la sécurité des TI. Les conclusions du centre d'évaluation enregistrées dans le rapport technique d'évaluation sont cohérentes avec les éléments de preuve fournis.

Ce certificat ne constitue pas en soi une recommandation du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise. Ce certificat n'exprime directement ou indirectement aucune caution du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

Secrétariat Général de la Défense Nationale
DCSSI
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du produit “Micro-circuit ATMEL AT90SC6464C (référence AT568A9 rév. F)”.

2 Le niveau d’assurance atteint est le niveau EAL1 augmenté du composant d’assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [CC-3].

3 Le micro-circuit est destiné à être inséré dans un support plastique pour constituer une carte à puce. Les usages de cette carte sont ensuite multiples (applications bancaires, de télévision à péage, de transport, de santé,...) en fonction des logiciels applicatifs qui y seront embarqués.

Chapitre 2

Résumé

2.1 Contexte de l'évaluation

4 L'évaluation a été menée conformément aux Critères Communs ([CC-1] à [CC-3]) et à la méthodologie définie dans le manuel CEM [CEM].

5 Elle s'est déroulée consécutivement au développement du produit de mars à juillet 2001.

6 Le commanditaire de l'évaluation (ci-après "le commanditaire") est ATMEL Smart Card ICs :

- ATMEL Smart Card ICs
  Maxwell Building
  Scottish Enterprise Technology Park
  East Kilbride, G75 0QF
  Ecosse

7 Le micro-circuit est développé sur le site d'ATMEL RFO à Rousset (France) :

- ATMEL RFO
  Z.I. Rousset Peynier
  13106 Rousset Cedex
  France

8 Le micro-circuit est fabriqué sur les sites d'ATMEL RFO à Rousset (France) et ATMEL GFO à Grenoble (France) :

- ATMEL RFO
  Z.I. Rousset Peynier
  13106 Rousset Cedex
  France

- ATMEL GFO
  Avenue de Rochepleine - BP123
  38521 St Egrève
  France

9 L'évaluation a été conduite par le Centre d'Evaluation de la Sécurité des Technologies de l'Information CEACI (ci-après "l'évaluateur") :

- CEACI (THALES Microelectronics-CNES)
  18 avenue Edouard Belin

31441 Toulouse Cedex
France

2.2 Description de la cible d'évaluation

10 La cible d'évaluation est le produit "Micro-circuit ATMEL AT90SC6464C (référence AT568A9 rév. F)".

11 Le micro-circuit est destiné à être inséré dans un support plastique pour constituer une carte à puce. Les usages de cette carte sont ensuite multiples (applications bancaires, de télévision à péage, de transport, de santé,...) en fonction des logiciels applicatifs qui y seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

12 Le détail des fonctions de sécurité évaluées résumées ci-après est disponible dans la cible de sécurité [ST] :

- Contrôle du passage en mode TEST,
- Contrôle d'accès aux mémoires en mode TEST,
- Blocage du mode TEST,
- Test du micro-circuit,
- Détection d'erreurs mémoire,
- Contrôle d'accès aux mémoires en exploitation,
- Détection d'évènements de sécurité,
- Réaction aux évènements de sécurité,
- Non-observabilité des opérations réalisées par le micro-circuit,
- Opérations cryptographiques (DES, TDES, SHA-1, RSA sans CRT, générateur de nombres aléatoires).

2.3 Conclusions de l'évaluation

13 Le produit soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [CC-3].

14 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL1 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élémentaire tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.

15 L'utilisation de la cible d'évaluation de manière sûre est soumise aux recommandations figurant au chapitre 6 du présent rapport.

Chapitre 3

Identification de la cible d'évaluation

3.1 Objet

15 La cible d'évaluation est le micro-circuit ATMEL AT90SC6464C (référence AT568A9 rév. F).

16 Ce micro-circuit est destiné à recevoir les logiciels fournis par des développeurs d'applications. Ces logiciels applicatifs sont chargés en mémoire Flash ou en EEPROM. Ces logiciels applicatifs ne font pas partie de l'évaluation.

17 Pour la présente évaluation, seul le chargement des applications pendant la phase de test réalisée par ATMEL GFO est autorisé.

18 Le micro-circuit est ensuite inséré dans une carte porteur de format carte de crédit ou tout autre support.

19 Les modes d'utilisation de la cible d'évaluation identifiés dans la cible de sécurité sont les suivants :

- mode Test : mode de test uniquement actif en phase de production du micro-circuit et dans un environnement sécurisé.
- mode User : mode normal d'utilisation.

3.2 Cycle de vie de la cible d'évaluation

20 Le cycle de vie de la cible d'évaluation est constitué des phases suivantes :

- phase 1 : développement des applications destinées à être chargées sur le micro-circuit,
- phase 2 : développement du micro-circuit,
- phase 3 : production du micro-circuit et chargement des applications,
- phase 4 : mise en micro-modules (ateliers de micro-électronique),
- phase 5 : encartage,
- phase 6 : personnalisation,
- phase 7 : utilisation du produit final.

21 Les phases 2 et 3 constituent les phase de construction de la cible d'évaluation.

22 Les phases 4 à 7 sont les phases d'exploitation de la cible d'évaluation.

3.3 Historique du développement

23 Le micro-circuit AT90C6464C a été développé par ATMEL RFO sur le site de Rousset (France).

24 La production des micro-circuits est réalisée sur le site d'ATMEL RFO à Rousset (France) et d'ATMEL GFO à Grenoble (France).

3.4 Description des matériels

25 Le micro-circuit AT90SC6464C fait partie de la famille de micro-circuits HERCULE développés par ATMEL Smart Card ICs. Ces micro-circuits sont bâtis autour des micro-contrôleurs de type AVR RISC.

26 Le micro-circuit AT90SC6464C dispose de :

- 64Ko de mémoire Flash,
- 8Ko de mémoire ROM,
- 3Ko de mémoire RAM,
- 64Ko de mémoire EEPROM.

27 Le micro-circuit AT90SC6464C contient un générateur de nombres aléatoires, un module DES/TDES matériel et un processeur cryptographique avec sa librairie logicielle.

3.5 Description des logiciels

28 Pour l'évaluation, le micro-circuit contient les logiciels suivants :

- un logiciel permettant de charger des applications de test. Ce logiciel est hors du champs de l'évaluation,
- la librairie standard du processeur cryptographique.

3.6 Description de la documentation

29 La documentation disponible pour l'utilisation du micro-circuit est la suivante :

a) la «technical Datasheet» :

- AT90SC6464C technical datasheet, réf. 1332 rev. D, 9 fév. 2001.

b) le guide de programmation :

- AT90SC Addressing Modes & Instruction Set, réf. 1323 rev. B, 26 fév. 2001.

c) les notes d'applications (Application Notes) :

- Application note : Toolbox v1.0 SC16 Crypto-coprocessor Library, réf. TPR0024A rev. 1.0, 13 fév. 2001.
- Application Note : Secured Hardware DES/TDES in the AT90SC6464C, réf. TPR0041A, 27 avril 2001.
- Application Note : Checksum accelerator use on the AT90SC6464C, réf. TPR0042A, 26 avril 2001.
- Application Note : Generating Unpredictable Random Numbers with the AT90SCxx, réf. TPR0037A, 27 avril 2001.
- Application Note : Securing the RSA operations in the AT90SC6464C, réf. TPR0040B, 4 juillet 2001.

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

20 Les caractéristiques de sécurité évaluées sont décrites dans la cible de sécurité [ST] qui est la référence pour l'évaluation. Les paragraphes ci-après reformulent les éléments essentiels de ces caractéristiques.

4.2 Hypothèses

21 La cible d'évaluation doit être utilisée dans un environnement qui satisfait aux hypothèses énoncées dans la cible de sécurité [ST].

22 Ces hypothèses sont les suivantes :

- les applications destinées à être chargées sur le micro-circuit sont protégées pendant leur phase de développement,
- les mesures de sécurité de l'environnement de développement et de fabrication des micro-circuits sont suffisantes pour protéger les micro-circuits et leurs informations de développement et de test,
- les micro-circuits et les informations associées sont protégés lors des phases d'encartage et de personnalisation et lors de leurs livraisons entre ces phases et l'utilisation finale,
- les terminaux et les protocoles utilisant les données sensibles du micro-circuit les protègent de manière adéquate.

4.3 Biens à protéger

23 Les biens à protéger par la cible d'évaluation sont les suivants :

- les données des applications,
- les logiciels embarqués,
- les informations de développement du micro-circuit,
- le micro-circuit lui-même.

4.4 Menaces

24 Les menaces suivantes couvertes par la cible d'évaluation ou par son environnement sont celles définies dans la cible de sécurité [ST] :

- modification non autorisée de la conception du circuit et des données applicatives du micro-circuit,

- divulgation non autorisée de la conception du circuit, des données applicatives du micro-circuit, des informations de tests et des outils de développement.

4.5 Politiques de sécurité organisationnelles

25 Aucune politique de sécurité organisationnelle n'est identifiée dans la cible de sécurité [ST].

4.6 Fonctions de sécurité évaluées

26 Les fonctions de sécurité évaluées sont listées dans la cible de sécurité [ST]. Ces fonctions de sécurité sont les suivantes :

- Contrôle du passage en mode TEST,
- Contrôle d'accès aux mémoires en mode TEST,
- Blocage du mode TEST,
- Test du micro-circuit,
- Détection d'erreurs mémoire,
- Contrôle d'accès aux mémoires en exploitation,
- Détection d'évènements de sécurité,
- Réaction aux évènements de sécurité,
- Non-observabilité des opérations réalisées par le micro-circuit,
- Opérations cryptographiques (DES, TDES, SHA-1, RSA sans CRT, générateur de nombres aléatoires).

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

28 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [RTE].

5.2 Principaux résultats de l'évaluation

29 Le produit soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [CC-3].

5.2.1 ASE : Evaluation de la cible de sécurité

30 Les critères d'évaluation sont définis par les sections ASE_DES.1.iE, ASE_ENV.1.iE, ASE_INT.1.iE, ASE_OBJ.1.iE, ASE_PPC.1.iE, ASE_REQ.1.iE, ASE_SRE.1.iE et ASE_TSS.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

31 La cible de sécurité [ST] rassemble l'ensemble des caractéristiques de sécurité de la cible d'évaluation. L'évaluateur s'est assuré que cette cible de sécurité décrit de manière suffisamment claire la cible d'évaluation, l'environnement supposé d'exploitation ainsi que les fonctions de sécurité évaluées.

32 Toutes les exigences fonctionnelles identifiées dans la cible de sécurité sont extraites de la partie 2 des Critères Communs [CC-2].

5.2.2 ACM_CAP.1 : Numéros de version

33 Les critères d'évaluation sont définis par la section ACM_CAP.1.iE de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

34 La cible d'évaluation est le micro-circuit AT90SC6464C développé par ATMEL Smart Card ICs.

35 La référence interne des réticules utilisés est AT568A9 révision F.

5.2.3 ADV_FSP.1 : Spécifications fonctionnelles informelles

36 Les critères d'évaluation sont définis par les sections ADV_FSP.1.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [CC-3].

37 Le développeur a fourni les spécifications des fonctions de sécurité du micro-circuit. Les interfaces externes de ces fonctions y sont également décrites.

38 L'évaluateur a examiné ces spécifications et montré pour le niveau considéré qu'elles représentent une description complète et homogène des fonctionnalités de sécurité du produit.

5.2.4 ADV_RCR.1 : Démonstration de correspondance informelle

39 Les critères d'évaluation sont définis par la section ADV_RCR.1.1E de la classe ADV, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

40 Le développeur a fourni une documentation indiquant la correspondance entre les fonctions de sécurité telles qu'elles sont définies dans les spécifications fonctionnelles (ADV_FSP) et la cible de sécurité (ASE_TSS).

41 L'évaluateur s'est assuré que les spécifications fonctionnelles correspondent à une image complète et cohérente des fonctions de sécurité décrites dans la cible de sécurité.

5.2.5 ADO_IGS.1 : Procédures d'installation, de génération et de démarrage

42 Les critères d'évaluation sont définis par les sections ADO_IGS.1.iE de la classe ADO, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

43 Aucune procédure d'installation n'est nécessaire pour un micro-circuit. La procédure de démarrage correspond au "reset".

44 L'évaluateur s'est assuré que ces procédures documentées permettent un démarrage sûr du micro-circuit.

5.2.6 AGD_ADM.1 : Guide de l'administrateur

45 Les critères d'évaluation sont définis par la section AGD_ADM.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

46 L'administration de la TOE concerne les opérations réalisées lors de la phase de tests avant l'envoi des micro-circuits aux clients.

47 L'évaluateur s'est assuré de l'absence d'incohérence dans la documentation fournie aux administrateurs et a vérifié que ces procédures permettent une administration sûre du produit.

5.2.7 AGD_USR.1 : Guide de l'utilisateur

48 Les critères d'évaluation sont définis par la section AGD_USR.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

49 Le développeur a fourni la documentation d'utilisation des fonctions de sécurité du micro-circuit. Ces guides contiennent un ensemble de recommandations à

destination des développeurs d'applications pour le micro-circuit. La liste est précisée au chapitre 3 du présent rapport de certification.

50 L'évaluateur s'est assuré que cette documentation permettait une utilisation sûre des fonctions de sécurité offertes par le micro-circuit.

5.2.8 ATE_IND.1 : Tests indépendants - Conformité

51 Les critères d'évaluation sont définis par les sections ATE_IND.1.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

52 L'évaluateur a effectué des tests fonctionnels sur le produit afin de vérifier la conformité des fonctions de sécurité par rapport à leurs spécifications.

5.2.9 AVA_VLA.2 : Analyse de vulnérabilités indépendante

53 Les critères d'évaluation sont définis par les sections AVA_VLA.2.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

54 Le développeur a fourni une analyse des vulnérabilités potentielles du produit.

55 L'évaluateur a examiné cette fourniture et réalisé sa propre analyse de vulnérabilités indépendante. Il a également réalisé des tests de pénétration afin de vérifier que le produit résiste aux attaques correspondant à un potentiel d'attaque élémentaire tel que défini par le composant AVA_VLA.2 "Analyse de vulnérabilités indépendante".

5.2.10 Verdicts

56 Pour tous les aspects des Critères Communs identifiés ci-dessus, un avis "réussite" est émis.

Chapitre 6

Recommandations d'utilisation

79 La cible d'évaluation "Micro-circuit ATMEL AT90SC6464C (référence AT568A9 rév. F)" est soumise aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

a) Le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [ST].

b) Les applications destinées à être installées sur le micro-circuit doivent impérativement respecter les guides d'utilisation émis par ATMEL Smart Card ICs et notamment les recommandations de programmation qui y figurent. La liste de ces documents est précisée au chapitre 3 du présent rapport de certification.

Chapitre 7

Certification

7.1 Objet

80 Le produit soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 «Analyse de vulnérabilités indépendante» tel que décrit dans la partie 3 des Critères Communs [CC-3].

81 Les exigences fonctionnelles auquelles répondent les fonctions de sécurité du produit sont toutes extraites de la partie 2 des Critères Communs [CC-2].

82 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL1 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élémentaire tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.

7.2 Portée de la certification

83 La certification ne constitue pas en soi une recommandation du produit. Elle ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle que des vulnérabilités exploitables n'aient pas été découvertes ; probabilité d'autant plus faible que le niveau d'assurance est élevé.

84 Le certificat ne s'applique qu'à la version évaluée du produit identifiée au chapitre 3.

85 La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	L'addition d'un ou de plusieurs composants d'assurance de la Partie 3 à un EAL ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou son environnement.
Cible d'évaluation	Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
EEPROM	Mémoire programmable et effaçable électriquement.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Flash	Type de mémoire réinscriptible électriquement.
Niveau d'assurance de l'évaluation (EAL)	Un paquet composé de composants d'assurance tirées de la Partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Une expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Politique de sécurité organisationnelle	Une ou plusieurs règles, procédures, codes de conduite ou lignes directrices de sécurité qu'une organisation impose pour son fonctionnement.
Produit	Un ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.

Profil de protection	Un ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.
Reset	Mise sous tension du micro-circuit.

Annexe B

Références

[CC-1] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 1 : Introduction et modèle général CCIMB-99-031, version 2.1 Août 1999.

[CC-2] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 2 : Exigences fonctionnelles de sécurité CCIMB-99-032, version 2.1 Août 1999.

[CC-3] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 3 : Exigences d'assurance de sécurité CCIMB-99-033, version 2.1 Août 1999.

[CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information Partie 2 : Méthodologie d'évaluation CEM-99/045, version 1.0 Août 1999.

[PP/9806] Profil de Protection PP/9806 "Smartcard Integrated Circuit", version 2.0, septembre 1998.

[ST] Cible de sécurité «HERCULE Security Target v. 1.2», réf. HER_ST_v1.2, ATMEL Smart Card ICs, 23 mai 2001.

[RTE] Rapport Technique d'Evaluation, réf. HER_RTE rév. 1.1, CEACI, 26 juillet 2001 (diffusion contrôlée).